THE GENUS FIELDS OF ARTIN-SCHREIER EXTENSIONS

SU HU AND YAN LI

Abstract. Let q be a power of a prime number p. Let $k = \mathbb{F}_q(t)$ be the rational function field with constant field $\mathbb{F}_q$. Let $K = k(\alpha)$ be an Artin-Schreier extension of k. In this paper, we explicitly describe the ambiguous ideal classes and the genus field of K . Using these results we study the p-part of the ideal class group of the integral closure of $\mathbb{F}_q[t]$ in K. And we also give an analogy of Rédei-Reichardt's formulae for K.

1. Introduction

In 1951, Hasse [6] introduced genus theory for quadratic number fields which is very important for studying the ideal class groups of quadratic number fields. Later, Fröhlich [3] generalized this theory to arbitrary number fields. In 1996, S.Bae and J.K.Koo [2] defined the genus field for global function fields and developed the analogue of the classical genus theory. In 2000, Guohua Peng [7] explicitly described the genus theory for Kummer function fields.

The genus theory for function fields is also very important for studying the ideal class groups of function fields. Let l be a prime number and K be a cyclic extension of degree l of the rational function field $\mathbb{F}_q(t)$ over a finite field of characteristic $\neq l$. In 2004, Wittmann [12] generalized Guohua Peng's results to the case $l \nmid q-1$ and used it to studied the l part of the ideal class group of the integral closure of $\mathbb{F}_q[t]$ in K following an ideal of Gras [4].

Let q be a power of a prime number p. Let $k = \mathbb{F}_q(t)$ be the rational function field with constant field $\mathbb{F}_q$. Assume that the polynomial $T^p - T - D \in k(T)$ is irreducible. Let $K = k(\alpha)$ with $\alpha^p - \alpha = D$. K is called an Artin-Schreier extension of k (See [5]). It is well known that every cyclic extension of $\mathbb{F}_q(t)$ of degree p is an Artin-Schreier extension. In this paper, we explicitly describe the genus field of K. Using this result we also study the p-part of the ideal class group of the integral closure of $\mathbb{F}_q[t]$ in K. Our results combined with Wittmann [12]'s results give the complete results for genus theory of cyclic extensions of prime degree over rational function fields.

Let O_K be the integral closure of $\mathbb{F}_q[t]$ in K. Let $Cl(K)$ be the ideal class group of the Dedekind domain O_K. Let $G(K)$ be the genus field of K. Our paper

2000 *Mathematics Subject Classification.* 11R58.
Key words and phrases. genus field, Artin-Schreier extension.

is organized as follows. In Section 2, we recall the arithmetic of Artin-Schreier extensions. In Section 3, we recall the definition of $G(K)$ and compute the ambiguous ideal classes of $Cl(K)$ using cohomological methods. As a corollary, we obtain the the order of $\mathrm{Gal}(G(K)/K)$. In Section 4, we described explicitly $G(K)$. In Section 5, we study the p-part of $Cl(K)$. And we also give an analogy of R*é*dei-Reichardt's formulae [10] for K.

2. The arithmetic of Artin-Schreier extensions

Let q be a power of a prime number p. Let $k = \mathbb{F}_q(t)$ be the rational function field. Let K/k be a cyclic extension of degree p. Then K/k is an Artin-Schreier extension, that is, $K = k(\alpha)$, where $\alpha^p - \alpha = D,\ D \in \mathbb{F}_q(t)$ and D can not be written as $x^p - x$ for any $x \in k$. Conversely, for any $D \in \mathbb{F}_q(t)$ and D can not be written as $x^p - x$ for any $x \in k$, $k(\alpha)/k$ is a cyclic extension of degree p, where $\alpha^p - \alpha = D$. Two Artin-Schreier extensions $k(\alpha)$ and $k(\beta)$ such that $\alpha^p - \alpha = D$ and $\beta^p - \beta = D'$ are equal if and only if they satisfy the following relations,

$$\begin{aligned} &\alpha \to x\alpha + B_0 = \beta, \\ &D \to xD + (B_0^p - B_0) = D', \\ &x \in \mathbb{F}_p^*, B_0 \in k. \end{aligned}$$

(See [5] or Artin [1] p.180-181 and p.203-206) Thus we can normalize D to satisfy the following conditions,

$$D = \sum_{i=1}^{m} \frac{Q_i}{P_i^{e_i}} + f(t),$$
$$(P_i, Q_i) = 1, \ \text{ and } p \nmid e_i, \ \text{for } 1 \le i \le m,$$
$$p \nmid \deg(f(t)), \ \text{if } f(t) \notin \mathbb{F}_q,$$

where $P_i (1 \le i \le m)$ are monic irreducible polynomials in $\mathbb{F}_q[t]$ and $Q_i (1 \le i \le m)$ are polynomials in $\mathbb{F}_q[t]$ such that $\deg(Q_i) < \deg(P_i^{e_i})$. In the rest of this paper, we always assume D has the above normalized forms and denote $\frac{Q_i}{P_i^{e_i}} = D_i$, for $1 \le i \le m$. The infinite place $(1/t)$ is splitting, inertial, or ramified in K respectively when $f(t) = 0$; $f(t)$ is a constant and the equation $x^p - x = f(t)$ has no solutions in $\mathbb{F}_q$; $f(t)$ is not a constant. Then the field K is called real, inertial imaginary, or ramified imaginary respectively. The finite places of k which are ramified in K are $P_1, \cdots, P_m$ (p.39 of [5]).Let $\mathfrak{P}_i$ be the place of K lying above $P_i (1 \le i \le m)$.

Let P be a finite place of k which is unramified in K. Let $(P, K/k)$ be the Artin symbol at P. Then

$$(P, K/k)\alpha = \alpha + \{\frac{D}{P}\}$$

and the Hasse symbol $\{\frac{D}{P}\}$ is determined by the following equalities:

$$\begin{aligned}
\{\frac{D}{P}\} &\equiv D + D^p + \cdots D^{N(P)/p} \text{mod } P \\
&\equiv (D + D^p + \cdots D^{N(P)/p}) \\
&+ (D + D^q + \cdots D^{N(P)/q})^p \\
&+ \cdots \\
&+ (D + D^q + \cdots D^{N(P)/q})^{q/p} \text{mod } P, \\
\{\frac{D}{P}\} &= \mathrm{tr}_{\mathbb{F}_q/\mathbb{F}_p} \mathrm{tr}_{(O_K/P)/\mathbb{F}_q}(D) \text{ mod P}
\end{aligned}$$

(p.40 of [5]).

3. Ambiguous ideal classes

From this point, we will use the following notations:

q – power of a prime number p.
k – the rational function field $\mathbb{F}_q(t)$.
K – an Artin-Schreier extension of k of degree p.
G – the Galois group $Gal(K/k)$.
σ – the geneartor of $Gal(K/k)$.
S – the set of infinite places of K (i.e, the primes above $(1/t)$).
O_K – the integral closure of $\mathbb{F}_q[t]$ in K.
$I(K)$ – the group of fractional ideals of O_K.
$P(K)$ – the group of principal fractional ideals of O_K.
$P(k)$ – the subgroup of $P(K)$ generated by nonzero elements of $\mathbb{F}_q(t)$.
$Cl(K)$ – the ideal class group of O_K.
$H(K)$ – the Hibert class field of K.
$G(K)$ – the genus field of K.
U_K – the unit group of O_K.

Definition 3.1. (Rosen [8])The Hilbert class field $H(K)$ of K (relative to S) is the maximal unramified abelian extension of K such that every infinite places (i.e. $\in S$) of K split completely in $H(K)$.

Definition 3.2. (Bae and Koo [2]) The genus field $G(K)$ of K is the maximal abelian extension of K in $H(K)$ which is the composite of K and some abelian extension of k.

For any G-module M, let M^G be the G-module of elements of M fixed by the action of G. Without lost of generality, we will assume K/k is a geometric extension in the rest of this paper. We have the following Theorem.

Theorem 3.3. *The ambiguous ideal classes $Cl(K)^G$ is a vector space over $\mathbb{F}_p$ generated by by $[\mathfrak{P}_1], [\mathfrak{P}_2], \cdots, [\mathfrak{P}_m]$ with dimension*

$$dim_{\mathbb{F}_p} Cl(K)^G = \begin{cases} m-1 & K \text{ is real}. \\ m & K \text{ is imaginary}. \end{cases}$$

Before the proof of the above theorem, we need some lemmas.

Lemma 3.4. $H^1(G, P(K)) = 1$.

Proof. From the following exact sequence

$$1 \longrightarrow U_K \longrightarrow K^* \longrightarrow P(K) \longrightarrow 1,$$

we have

$$1 \longrightarrow H^1(G, P(K)) \longrightarrow H^2(G, U_K) \longrightarrow H^2(G, K^*) \longrightarrow \cdots$$

This is because K/k is a cyclic extension and $H^1(G, K^*) = 1$ (Hilbert Theorem 90). Since

$$H^2(G, U_K) = \frac{U_K^G}{NU_K} = \frac{\mathbb{F}_q^*}{(\mathbb{F}_q^*)^p} = 1, \tag{3.1}$$

we have $H^1(G, P(K)) = 1$. □

Lemma 3.5. *If K is imaginary, then* $H^1(G, U_K) = 1$.

Proof. Since $U_K = \mathbb{F}_q^*$, we have

$$H^1(G, \mathbb{F}_q^*) = \frac{\{x \in \mathbb{F}_q^* | x^p = 1\}}{\{x^{\sigma-1} | x \in \mathbb{F}_q^*\}} = 1.$$

□

Lemma 3.6. *If K is real, then* $H^1(G, U_K) \cong \mathbb{F}_p$.

Proof. We denote by $\mathscr{D}$ the group of divisors of K, by $\mathscr{P}$ the subgroup of principal divisors. We define $\mathscr{D}(S)$ to be the subgroup of $\mathscr{D}$ generated by the primes in S and $\mathscr{D}^0(S)$ to be the degree zero divisors of $\mathscr{D}(S)$. From Proposition 14.1 of [9], we have the following exact sequence

$$(0) \longrightarrow \mathbb{F}_q^* \longrightarrow U_K \longrightarrow \mathscr{D}^0(S) \longrightarrow Reg \longrightarrow (0),$$

where the map from U_K to $\mathscr{D}^0(S)$ is given by taken an element of U_K to its divisor and Reg is a finite group (See Proposition 14.1 and Lemma 14.3 of [9]). By Proposition 7 and Proposition 8 of [11] (p.134), we have $h(U_K) = h(\mathscr{D}^0(S))$,

where $h(*)$ is the Herbrand Quotient of $*$. By Equation (3.1), we have $H^2(G, U_K) = 1$. Thus, we can prove this Lemma by showing $h(\mathscr{D}^0(S)) = 1/p$.

Let ∞ be any infinite place in S. Thus $\mathscr{D}^0(S)$ is the free abelian group generated by $(\sigma-1)\infty, (\sigma^2-\sigma)\infty, \cdots, (\sigma^{p-1}-\sigma^{p-2})\infty$. And we have

$$\mathscr{D}^0(S) = \mathbb{Z}[G](\sigma-1)\infty \cong \frac{\mathbb{Z}[G]}{(1+\sigma+\cdots\sigma^{p-1})}. \tag{3.2}$$

Let ζ_p be a p-th root of unity. We have

$$\frac{\mathbb{Z}[G]}{(1+\sigma+\cdots\sigma^{p-1})} \cong \mathbb{Z}[\zeta_p], \tag{3.3}$$

and the above map is given by taken σ to ζ_p. From (3.2) and (3.3), we have

$$\begin{aligned} H^1(G, \mathscr{D}^0(S)) &= \frac{kerN\mathscr{D}^0(S)}{(\sigma-1)\mathscr{D}^0(S)} = \frac{\mathscr{D}^0(S)}{(\sigma-1)\mathscr{D}^0(S)} \\ &\cong \frac{\frac{\mathbb{Z}[G]}{(1+\sigma+\cdots\sigma^{p-1})}}{(\sigma-1)\frac{\mathbb{Z}[G]}{(1+\sigma+\cdots\sigma^{p-1})}} \cong \frac{\mathbb{Z}[\zeta_p]}{(\zeta_p-1)} \cong \mathbb{F}_p \end{aligned}$$

and

$$H^2(G, \mathscr{D}^0(S)) = \frac{\mathscr{D}^0(S)^G}{N\mathscr{D}^0(S)} = 0.$$

Thus $h(\mathscr{D}^0(S)) = 1/p$. □

Proof of Theorem 3.3: From the following exact sequence

$$1 \longrightarrow P(K) \longrightarrow I(K) \longrightarrow Cl(K) \longrightarrow 1,$$

we have

$$1 \longrightarrow P(K)^G \longrightarrow I(K)^G \longrightarrow Cl(K)^G \longrightarrow H^1(G, P(K)) \longrightarrow \cdots$$

Since $H^1(G, P(K)) = 1$ by Lemma 3.4, we have

$$1 \longrightarrow P(K)^G \longrightarrow I(K)^G \longrightarrow Cl(K)^G \longrightarrow 1.$$

Thus

$$1 \longrightarrow \frac{P(K)^G}{P(k)} \longrightarrow \frac{I(K)^G}{P(k)} \longrightarrow Cl(K)^G \longrightarrow 1. \tag{3.4}$$

From the following exact sequence

$$1 \longrightarrow U_K \longrightarrow K^* \longrightarrow P(K) \longrightarrow 1,$$

we have

$$1 \longrightarrow \mathbb{F}_q^* \longrightarrow k^* \longrightarrow P(K)^G \longrightarrow H^1(G, U_K) \longrightarrow 1$$

and

$$H^1(G, U_K) \cong \frac{P(K)^G}{P(k)}. \tag{3.5}$$

Since $\frac{I(K)^G}{P(k)}$ is a vector space over $\mathbb{F}_p$ with basis $[\mathfrak{P}_1], [\mathfrak{P}_2], \cdots, [\mathfrak{P}_m]$, by (3.4), (3.5), Lemma 3.5 and Lemma 3.6, we get the desired result.

Remark 3.7. If K is real, it is an interesting question to find explicitly the relation satisfied by $[\mathfrak{P}_1], [\mathfrak{P}_2], \cdots, [\mathfrak{P}_m]$ in $Cl(K)^G$. By Lemma 3.5, if we can find a nontrivial element $\bar{u}$ of $H^1(G, U_K)$, then by Hibert 90, we have $u = x^{\sigma-1}$, where $u \in U_K$ and $x \in K$. It is easy to see that

$$\sum_{i=1}^{m} ord_{\mathfrak{P}_i}(x)[\mathfrak{P}_i] = 0$$

in $Cl(K)^G$.

From Proposition 2.4 of [2], we have

$$Gal(G(K)/K) \cong Cl(K)/(\sigma - 1)Cl(K) \cong Cl(K)^G. \tag{3.6}$$

(It should be noted that the last isomorphism is merely an isomorphism of abelian groups but not canonical). Therefore, we get

Corollary 3.8.

$$\#Gal(G(K)/K) = \begin{cases} p^{m-1} & K \text{ is real.} \\ p^m & K \text{ is imaginary.} \end{cases}$$

4. The genus field $G(K)$

In this section, we prove the following theorem which is the main result of this paper.

Theorem 4.1.

$$G(K) = \begin{cases} k(\alpha_1, \alpha_2, \cdots, \alpha_m) & K \text{ is real.} \\ k(\beta, \alpha_1, \alpha_2, \cdots, \alpha_m) & K \text{ is imaginary.} \end{cases}$$

Where $\alpha_i^p - \alpha_i = D_i = \frac{Q_i}{P_i^{e_i}} (1 \leq i \leq m), \beta^p - \beta = f(t)$, *and* $D_i, Q_i, P_i, f(t)$ *are defined in Section 2.*

We only prove the imaginary case. The proof is the same for the real case. Since

$$\left(\sum_{i=1}^{m} \alpha_i + \beta\right)^p - \left(\sum_{i=1}^{m} \alpha_i + \beta\right) = \sum_{i=1}^{m} \frac{Q_i}{P_i^{e_i}} + f(t) = D,$$

we can assume $\alpha = \sum_{i=1}^{m} \alpha_i + \beta$. Before the proof of the above theorem, we need two lemmas.

Lemma 4.2. *$E = k(\beta, \alpha_1, \alpha_2, \cdots, \alpha_m)$ is an unramified abelian extension of K.*

Proof. Let P be a place of k and let $(1/t)$ be the infinite place of k. If $P \neq P_1, P_2, \cdots, P_m, (1/t)$, then P is unramified in $k(\beta), k(\alpha_i)(1 \leq i \leq m)$, hence unramified in E. Otherwise, without lost of generality, we can suppose $P = P_1$. Since $\alpha = \sum_{i=1}^{m} \alpha_i + \beta$, we have $E = Kk(\alpha_2, \cdots, \alpha_m, \beta)$. Thus $P = P_1$ is unramified in $k(\alpha_2, \cdots, \alpha_m, \beta)$, hence unramified in E/K. □

Lemma 4.3. *The infinite places of K are split completely in $E = k(\beta, \alpha_1, \alpha_2, \cdots, \alpha_m)$.*

Proof. Since $\alpha = \sum_{i=1}^m \alpha_i + \beta$, we have $E = Kk(\alpha_1, \alpha_2, \cdots, \alpha_m)$. Since the infinite place $(1/t)$ of k splits completely in $k(\alpha_1, \alpha_2, \cdots, \alpha_m)$, hence $(1/t)$ also splits completely in E/K. □

Proof of Theorem 4.1:From Lemma 4.2 and 4.3, we have

$$k(\alpha_1, \alpha_2, \cdots, \alpha_m, \beta) \subset G(K). \tag{4.1}$$

Comparing ramifications, $k(\beta), k(\alpha_i)(1 \leq i \leq m)$ are linearly disjoint over k, so

$$[k(\alpha_1, \alpha_2, \cdots, \alpha_m, \beta) : k] = p^{m+1}$$

and

$$[k(\alpha_1, \alpha_2, \cdots, \alpha_m, \beta) : K] = p^m.$$

Thus from Corollary 3.8 and (4.1), we get the result.

5. The p-part of $Cl(K)$

If l is a prime number, K is a cyclic extension of k of degree l, and $\mathbb{Z}_l$ is the ring of l-adic integers, then $Cl(K)_l$ is a finite module over the discrete valuation ring $\mathbb{Z}_l[\sigma]/(1 + \sigma + \cdots + \sigma^{l-1})$. Thus its Galois module structure is given by the dimensions:

$$\lambda_i = dim(Cl(K)_l^{(\sigma-1)^{i-1}} / Cl(K)_l^{(\sigma-1)^i})$$

for $i \geq 1$, these quotients being $\mathbb{F}_l$ vector spaces in a natural way. In number field situations, the dimensions λ_i have been investigated by Rédei [10] for $l = 2$ and Gras [4] for arbitrary l. In function field situations, these dimensions λ_i have been investigated by Wittmann for $l \neq p$. In this section, we give a formulae to compute λ_2 for $l = p$. This is an analogy of Rédei-Reichardt's formulae [10] for Artin-Schreier extensions.

If K is imaginary, as in the proof of Theorem 4.1, we suppose that $K = k(\alpha)$, where $\alpha = \sum_{i=1}^m \alpha_i + \beta$. We have the following sequence of maps

$$\begin{aligned} Cl(K)^G &\longrightarrow Cl(K)/(\sigma - 1)Cl(K) \cong Gal(G(K)/K) \hookrightarrow Gal(G(K)/k) \\ &\cong Gal(k(\alpha_1)/k) \times \cdots \times Gal(k(\alpha_m)/k) \times Gal(k(\beta)/k). \end{aligned}$$

Considering $[\mathfrak{P}_i] \in Cl(K)^G$ $(1 \leq i \leq m)$ under these maps, we have

$$\begin{aligned} [\mathfrak{P}_i] \longmapsto [\overline{\mathfrak{P}_i}] \longmapsto (\mathfrak{P}_i, G(K)/K) \longmapsto (\mathfrak{P}_i, G(K)/K) \\ \longmapsto ((P_i, k(\alpha_1)/k), \cdots, (P_i, k(\alpha_m)/k), (P_i, k(\beta)/k)), \end{aligned}$$

where the i-th component is $(\mathfrak{P}_i, G(K)/K)|_{k(\alpha_i)}$.

We define the Rédei matrix $R = (R_{ij}) \in M_{m\times m}(\mathbb{F}_p)$ as following:

$$R_{ij} = \{\frac{D_j}{P_i}\}, \text{ for } 1 \leq i, j \leq m, i \neq j,$$

and R_{ii} is defined to satisfy the equality:

$$\sum_{j=1}^{m} R_{ij} + \{\frac{f}{P_i}\} = 0.$$

From the discussions in section 2, we have

$$(\mathfrak{P}_i, G(K)/K)\alpha = \alpha,$$
$$(\mathfrak{P}_i, G(K)/K)\alpha_j = \alpha_j + \{\frac{D_j}{P_i}\}, for\ i \neq j$$
$$(\mathfrak{P}_i, G(K)/K)\beta = \beta + \{\frac{f}{P_i}\},$$

so it is easy to see the image of $Cl(K)^G \to Cl(K)/(\sigma-1)Cl(K)$ is isomorphic to the vector space generated by the row vectors $(R_{i1}, R_{i2}, \cdots, R_{im}, \{\frac{f}{P_i}\})$ $(1 \leq i \leq m)$.

We conclude that

$$\begin{aligned}\lambda_2 &= dim_{\mathbb{F}_p}(Cl(K)_l^{(\sigma-1)}/Cl(K)_l^{(\sigma-1)^2}) = dim_{\mathbb{F}_p}(Cl(K)^{(\sigma-1)}/Cl(K)^{(\sigma-1)^2})\\ &= dim_{\mathbb{F}_p} \ker(Cl(K)^G \to Cl(K)/(\sigma-1)Cl(K))\\ &= dim_{\mathbb{F}_p} Cl(K)^G - dim_{\mathbb{F}_p} Im(Cl(K)^G \to Cl(K)/(\sigma-1)Cl(K))\\ &= m - rank(R).\end{aligned}$$

Since the proof of real case is similar, we only give the results and sketch the proof.

If K is real, from the discussions in section 2, we have $f(t) = 0$, so

$$D = \sum_{i=1}^{m} D_i.$$

We define the Rédei matrix $R = (R_{ij}) \in M_{m\times m}(\mathbb{F}_p)$ as following:

$$R_{ij} = \{\frac{D_j}{P_i}\},\ \text{for } 1 \leq i, j \leq m, i \neq j,$$

and R_{ii} is defined to satisfy the equality:

$$\sum_{j=1}^{m} R_{ij} = 0.$$

The same procedure as the imaginary case shows that the image of $Cl(K)^G \to Cl(K)/(\sigma-1)Cl(K)$ is isomorphic to the vector spaces generated by the row vectors of Rédei matrix. Thus

$$\begin{aligned}\lambda_2 &= dim_{\mathbb{F}_p} Cl(K)^G - dim_{\mathbb{F}_p} Im(Cl(K)^G \to Cl(K)/(\sigma-1)Cl(K))\\ &= m - 1 - rank(R).\end{aligned}$$

Theorem 5.1. *If K is imaginary, then $\lambda_2 = m - rank(R)$; if K is real, then $\lambda_2 = m - 1 - rank(R)$, where R is the Rédei matrix defined above.*

If $p = 2$, then σ acting on $Cl(K)$ equal to -1. So λ_1, λ_2 equal to the 2-rank, 4-rank of ideal class group $Cl(K)$, respectively. In particular, the above theorem tells us the 4-rank of ideal class group $Cl(K)$ which is an analogue of classical Rédei-Reichardt's 4-rank formulae for narrow ideal class group of quadratic number fields.

References

[1] E.Artin, Algebraic numbers and algebraic functions, AMS CHELSEA PUBLISHING, 2005.

[2] S.Bae and J.K.Koo, Genus theory for function fields, J.Austral.Math.Soc.(Series A)60(1996),301-310.

[3] A.Fröhlich, Central extensions, Galois groups, and ideal classes of number fields, Contemp.Math.24(Amer.Math.Soc.Providence,1983).

[4] G.Gras, Sur les l-classes d'idéaux dans les extensions cycliques relatives de degré premier l I,II,Ann.Inst.Fourier 23(3)(1973)1-48;Ann.Inst.Fourier 23(4)(1973)45-64.

[5] H.Hasse, Theorie der relativ zyklischen algebraischen Funktionenköper, insbesondere bei endlichem Konstantenköper. J.Reine Angew.Math. 172(1934),37-54.

[6] H.Hasse, Zur Geschlecht Theorie in quadratisehe Zahlkörpern, J.Math.Soc.Japan 3(1951),45-51.

[7] G. Peng, The genus fields of Kummer function fields, J.Number Theory 98(2003), 221-227.

[8] M.Rosen, The Hilbert class field in function field, Exp.Math.5(1987), 365-378.

[9] M.Rosen, Number Theory in Function Fields, Springer-verlag, New York,2002.

[10] L.Rédei, Arithmetischer Beweis des Satzes uber die Anzahl der durch vier teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlköper, J.Reine Angew Math.171(1935) 55-60.

[11] J.P.Serre, Local fields, Springer-verlag, New York, 1979.

[12] C.Wittmann, *l*-class groups of cyclic function fields of degree *l*, Finite Fields Appl.13(2007), 327-347.

Department of Mathematical Sciences, Tsinghua University, Beijing 100084, China
E-mail address: hus04@mails.tsinghua.edu.cn, liyan_00@mails.tsinghua.edu.cn